

ALERT

THE NEWSLETTER FOR INFORMATION PROTECTION PROFESSIONALS

Number 224
October 2001COMPUTER
SECURITY
INSTITUTE
600 HARRISON STREET
SAN FRANCISCO
CALIFORNIA 94107
TEL: (415) 947-6320

INSIDE INFORMATION

 **Anti-Matter**
*Lew Koch interviews
Marc Maiffret on the
CodeRed discovery*

2

 **Tools & Techniques**
*Rik Farrow weighs in
convincingly on the
full disclosure debate*


4

 **Calendar of Events**
*The 28th. annual is
only weeks away—
sign up now*

7

 **Bonus Item**
*Establish backup out-
sourcing for mission-
critical services*

9

 **In Case You Missed It 10**
*Real-world tales
of digital woe
and mischief*

10

The road to Kabul has been under construction for awhile...

By Richard Power

I was born in New York City. I raised myself on its hard streets. Even after living in Northern California for over twenty years, I still consider myself a New Yorker.

I felt the tragedy of September 11, 2001 in a very personal way.

I am also a patriot, for better or worse. My father fought at Iwo Jima. Some of those I respect most in my professional life work in or around the Pentagon.

I believe Osama bin Laden bears responsibility for the carnage of that awful morning. I hope he meets the Great Spirit soon. I am certain the encounter will surprise him.

Nevertheless, there are some bitter lessons that the U.S. needs to learn.

If information were nourishment, and your sole source of sustenance were FOX News and White House press briefings you would starve to death.

Contrary to the prevailing political rhetoric and media hype, the world did not "change forever" on that awful morning. The "war" on terrorism has been going on for many years. Some dire warnings have gone unheeded, some vital recommendations have gone unimplemented. There have been successes as well as failures. Serious analysis, deep thinking and committed attempts to prepare for the inevitable have been underway for years. The chickens simply came home to roost.

Reactive measures, like military action, however warranted or necessary are not all that is demanded by the situation. There are many proactive measures (in regard to security and intelligence) that have already been thrashed out and simply need to be implemented with diligence and determination.

Some background and context buried under the rubble

For a reality check, I turned to Michael Zuckerman, a journalist who has covered terrorism, law enforcement and national security issues for twenty-five years. When I spoke with him he had just finished spending the first week after the attack as an adviser to *America's Most Wanted* for a two-hour TV special on terrorism.

"On the positive side, keep in mind that this was something like the tenth attempt by this particular terrorist network. The initial WTC bombing was supposed to have toppled one tower into the other. Sheik Omar Abdel-Rahman arrested in Brooklyn a couple years later was going to blow up all the bridges, tunnels, federal buildings and the UN. There was the foiled plot to simultaneously blow up several U.S. jumbo jets over the Pacific. Another half dozen people have been picked up with bombs. Many more were deported having come in on fake passports. It stood to reason that eventually they would succeed, until now they have failed due their own stupidity. Do you recall how the FBI unraveled the original WTC bombing? The terrorists went back to the truck rental shop in Jersey to get back their deposit on the bomb truck—which they reported stolen. Abdel-Rahman was nailed when neighbors complained to police about the stench (they thought there was someone dead in there) emanating from the apartment where the ter-

continued on page 8

rorists were mixing barrels of nitrate to make bombs. During the ramp up to the Gulf War, Saddam sent word to his terrorist cells around the world to make plans to slaughter Americans. Scores of them traveled the world, many with plastic explosives. They were all rounded up. Why? Saddam's military intelligence issued them all fake passports with sequential numbers! One did succeed in setting off a bomb, outside a US consulate in Indonesia. The terrorist was the only one killed."

Lessons of the recent past unlearned

On September 16, in a powerful essay for the *San Francisco Chronicle*, Abraham D. Sofaer, a Senior Fellow of the Hoover Institution at Stanford University exhorts us to "stop playing games with terrorists."

"U.S. Presidents are responsible. Instead of using the military to eliminate terrorist groups, they have relied on the FBI and federal prosecutors to investigate and try only those few low-level operatives we are fortunate to arrest.

According to Sofaer, an anti-terrorism policy "based on criminal prosecution" creates "the misleading impression that the U.S. government is providing the American people with meaningful protection."

"It is not," he concludes.

According to Sofaer, the September 11 terrorist attack, as well as other such incidents, succeeded because of "a reckless indifference to security standards."

"The U.S. military housing complex, Khobar Towers, near Dhahran, Saudia Arabia, and the U.S. Embassy in Nairobi, Kenya, lacked essential perimeter protection.

"Seventeen sailors were killed on the destroyer USS Cole while it was docked in Aden, Yemen, on October 12, 2000, when slipshod security allowed an unknown vessel to come close enough to blow a hole in its hull.

"The World Trade Center bombing in 1993 might have been prevented if Arabic-language documents seized earlier from terrorists had been translated."

Prior warnings and recommendations ignored

In 1998, Bill Clinton, then-U.S. President, and Newt Gingrich, then-Speaker of the House, established a truly bi-partisan commission of seven Democrats and seven Republicans led by former Senators, Warren Rudman (R-NH) and Gary Hart (D-CO) to look into National Security in the 21st Century.

In January 2001, the Rudman-Hart commission delivered their final report to the Bush-Cheney administration just taking over the White House.

Speaking to Jake Tapper, Washington correspondent for *Salon*, after the September 11 terrorist strike, former Senator Hart said, "We predicted it. We said Americans will likely die on American soil, possibly in large numbers..."

The Rudman-Hart report included recommendations for a sweeping reorganization of resources dedicated to the "homeland security" of the U.S.

But the Bush administration rejected the commission's recommendations, and announced in March that it would conduct its own study directed by Dick Cheney.

More than two years of important work down the drain?

Meanwhile, the emphasis of the new administration was on selling a "missile defense system" that would not have

helped in the least on that awful morning.

Rudman, Hart's co-chairman, spelled it out for Tapper.

"Had they adopted every recommendation we had put forward at that time I don't think it would have changed what happened. There wasn't enough time to enact everything..On the other hand, if two years go by and the same thing happens again, shame on everybody."

During a prime-time address to the nation, one week after the attack (several days after the Salon story), the President appointed Gov. Tom Ridge (R-PA.), to direct the "Office of Homeland Security."

"Today, dozens of federal departments and agencies, as well as state and local governments, have responsibilities affecting homeland security. These efforts must be coordinated at the highest level. So tonight, I announce the creation of a Cabinet-level position reporting directly to me, the Office of Homeland Security."

Neither the President's speech nor the Associated Press story on Ridge's appointment mentioned the previously rejected report that had recommended the creation of the Cabinet-level position and articulated its mission.

Bail-outs are okay, but tighter controls are not?

In 1997, then-Vice President Al Gore's "White House Commission on Aviation Safety and Security" delivered its final report, which included numerous substantive recommendations for improvements in airport security.

David Learmont of *Flight International* told the *London Times* that the U.S. airline industry had rejected the Gore commission's recommendations: "The airlines turned it down because they said aviation in America is like traveling on buses: people hop on and off. Everything is aimed at processing the largest number of passengers.

"The (Gore) commission had said that the internal flights should have the same, much higher level of security surrounding international flights. In Europe, the same level of security covers both domestic and international flights."

The Gore Commission estimated the cost of implementing all of its recommendations at somewhere between \$2.5 billion and \$8 billion (depending upon which technologies were used). But airline industry lobbied aggressively against the anti-terrorism regulations in the Senate and House of Representatives and it went nowhere. (And yes, the airline industry had contributed significantly to the re-election campaigns of lawmakers on the relevant committees.)

Ironically, on September 17, a week after the terrorist attack, the Bush administration proposed a comprehensive financial aid package for the U.S. airline industry to help it recover. The bail-out was not tied to acceptance of the Gore Commission recommendations. The Federal government itself will pay for \$3 billion in security upgrades out of the \$40 billion authorized for the "new" war of terrorism.

At least, the final package that passed both Houses of Congress included a freeze on executive-level salaries.

An estimated 100,000 airline employees have been laid off.

Information is power, unless you can't use it

In the Information Age, information is power—but it is useless unless it is organized, analyzed and acted upon.

continued on page 6

continued from page 8

According to the *Los Angeles Times*, a high-ranking law enforcement official acknowledges that the Mossad (Israel's intelligence agency) alerted the U.S., in August, that as many as 200 terrorists were slipping into this country and planning "a major assault on the U.S." involving a "large-scale target" in the U.S. and that Americans would be "very vulnerable."

According to Reuters and the French radio station Europe 1, the FBI arrested an Islamic militant in Boston in August and received French intelligence reports linking him to Osama bin Laden but "apparently did not act on them." The man had dual French and Algerian nationality who had several passports, technical information on Boeing aircraft and flight manuals and had been taking flying lessons, it added. French security services provided a dossier clearly identifying him as an Islamic militant working with bin Laden. "He has a pedigree as long as your arm, an investigator said," the radio reported. "He belongs to the Pakistani-Afghan network that trains Osama bin Laden's soldiers."

Reuters also reported that an Arab journalist with access to bin Laden said that the terrorist had warned three weeks before the event that his followers would conduct "an unprecedented attack on U.S. interests for its support of Israel."

"Abdel-Bari Atwan, editor of the London-based *al-Quds al-Arabi*, an Arabic-language weekly news magazine, said Islamic fundamentalists led by bin Laden were 'almost certainly' behind the attack of the World Trade Center.

"Personally we received information that he planned very, very big attacks against American interests. We received several warnings like this. We did not take it so seriously, preferring to see what would happen before reporting it."

According to *CNN*, the U.S. was warned in 1995 of a terrorist plot to hijack commercial planes and crash them into the Pentagon, the CIA headquarters, and commercial towers in New York, Chicago and San Francisco.

"Philippine authorities learned of the plot after a small fire in a Manila apartment, which turned out to be the hideout of Ramzi Yousef, who was later convicted for his role in the 1993 bombing of the World Trade Center. Yousef escaped at the time, but agents caught his right-hand man, Abdul Hakim Murad, who told them a chilling tale about a plan by the Ramzi cell in the continental U.S. to hijack a commercial plane and ram it into the CIA headquarters in Langley, Virginia, and also the Pentagon," said Rodolfo Mendoza, a Philippine intelligence investigator.

Chronic problem

Lack of information sharing, lack of coordination and cooperation between intelligence agencies and law enforcement is a chronic and well-documented problem. Commissions come and go, lobbyists stay on. It is not the fault of the investigators on the street, it is an organizational problem, and a political problem. And it must be dealt.

The Hart-Rudman commission's final reports underscored the problem and made specific recommendations in regard to information and intelligence.

"Good intelligence is the key to preventing attacks on the homeland and homeland security should become one of the intelligence community's most important missions. Better hu-

man intelligence must supplement technical intelligence, especially on terrorist groups covertly supported by states. As noted above, fuller cooperation and more extensive information-sharing with friendly governments will also improve the chances that would-be perpetrators will be detained, arrested, and prosecuted before they ever reach U.S. borders."

Gore's commission on air safety and security also took a hard look at these information and intelligence issues.

"Profiling can leverage an investment in technology and trained people. Based on information that is already in computer databases, passengers could be separated into a very large majority who present little or no risk, and a small minority who merit additional attention.

"First, FBI, CIA, and BATF should evaluate and expand the research into known terrorists, hijackers, and bombers needed to develop the best possible profiling system. They should keep in mind that such a profile would be most useful to the airlines if it could be matched against automated passenger information which the airlines maintain. Second, the FBI and CIA should develop a system that would allow important intelligence information on known or suspected terrorists to be used in passenger profiling without compromising the integrity of the intelligence or its sources. Third, the Commission will establish an advisory board on civil liberties questions that arise from the development and use of profiling systems."

A chain is only as strong as its weakest link

The September 11 terrorist attack was not high-tech, it was not "21st Century." Its primitivism was its genius.

The hijackers used to knives, box-cutters, brute force and intimidation to take over the four flights.

They did not smuggle plastic explosives on-board. The airplanes they commandeered and the buildings they targeted served as the components of a powerful explosive device. Their suicidal fanaticism was the detonator.

The human factor was critical to the success of the terrorists' crime against humanity. Without their own unflinching will to end their own lives in the ensuing catastrophe, the plan would not have succeeded.

Similarly, the human factor is critical in thwarting attacks.

Who is on the frontline at the check-in counters and the metal detectors of our airports? How well have they been trained? How heightened is their awareness? Are these people professionals? Could they connect the dots if the dots were there to connect?

A chain is only as strong as its weakest link.

On September 17, CBS News provided some answers.

"Besides low wages no benefits, and abuse from passengers, the hours are long and the work is tedious. At many airports, the annual turnover rate exceeds 100 percent. At Boston's Logan Airport, where two of the hijacked flights originated, the turnover rate was 200 percent.

"Last year, federal prosecutors indicted Argenbright Security for supplying applicants at Philadelphia International Airport with phony high school diplomas, falsifying test scores, and lying about background checks that were never conducted. Fourteen security screeners had been convicted of various felonies including aggravated assault, robbery, resisting arrest

and forgery. At Oakland International, procedures were so lax that even employees are embarrassed. All Daniello Worcullo and Kevin McCree had to do to get their jobs at Huntley Security was to watch videos for two days and take a test, true or false."

And on board the planes themselves? Remember the sky marshals? The collective will of the terrorists to do harm simply outlasted the collective will of industry and government to thwart them.

The fire next time

Indeed, the September 11 attack was successful in large part because of its primitivism. But in the aftermath of the tragedy airport security personnel are now searching passengers and baggage for razors, knives, etc. So what's next?

There are many ghastly possibilities—and yes, they include cyber-based terrorist attacks. The vulnerabilities of the air traffic control system are well-documented. Perhaps it is the next line of least resistance. Those who once used guns and plastic, and most recently used brute force and sharp objects, may well use computer keyboards next time.

Furthermore, if we are going down the slippery slope into a protracted struggle it is quite plausible that we will begin to see coordinated attacks on both physical and cyber targets—for example, bombings at airports in conjunction with cyber attacks on elements of the air traffic control system.

Sowing what you reap

The U.S. invasion of Panama to arrest strongman Manuel Noriega, as well as the U.S.-led Gulf War to reverse the Iraqi invasion of Kuwait resulted in many deaths (although not many U.S. body bags). And yet, both Noriega and Saddam Hussein had earlier been nurtured by the U.S. during the civil war in Nicaragua and Iraq's long war with Iran respectively. Similarly, both Osama bin Laden and the Afghani leadership, which shelters him, were nurtured by the U.S. for its own purposes during the Soviet invasion of Afghanistan. On September 11th, bin Laden and, indirectly, the Taliban, caused the death of thousands of innocent people on a single morning. What dangerous seed are we sowing now?

Conclusion

Clearly, there is more to be done (and undone) than launching military strikes and indulging in bombastic rhetoric. Comprehensive security (i.e., physical, cyber, and personnel) is still not given adequate attention; and the processes involved in intelligence gathering, analysis and dissemination are still outmoded. The world will probably not be free from the threat of such attacks for a long time, but there is much that could be done to mitigate that risk and thwart numerous attempts in the coming years—if the lessons of the past be learned and the recommendations of reasonable, informed statesmen are acted upon. If not, more time be lost and with it more lives.

For Hart-Rudman's U.S. Commission on National Security/21st Century report, go to www.mipt.org/srchnatlstrat03272001c.html#_ftnl.

For the Al Gore's White House Commission of Aviation Safety and Security report, go to www.fas.org/irp/threat/212fin~1.html



CALENDAR OF EVENTS

Major Meetings

28th Annual Security Conference & Exhibition

October 29-31, 2001, Washington, D.C.

NetSec 2002

June 17-19, 2002, San Francisco, CA.

Regional Seminars 2001

November

- Washington, D.C.**
- 1-2 How to Develop Information Security Standards and Procedures, Tom Peltier
- 1-2 Intrusion Techniques and Countermeasures, Rik Farrow
- 1-2 Technical Recovery of Electronic Evidence, Peter Garza
- 1-2 How to Develop a Winning Security Architecture, David Lynas
- 1-2 Internet Security Tools and Techniques, Fred Avolio
- 1-2 Windows 2000 Security, Joel Scambray
- 1-2 Securing E-Business: A Technical Guide to Implementing PKI, Anish Bhimani
- San Francisco, CA**
- 12-13 How to Develop Information Security Policies, Tom Peltier
- 14-15 How to Develop Information Security Standards and Procedures, Tom Peltier
- Gaithersburg, MD**
- 27-28 How to Create & Sustain a Quality Info Security Awareness Program, John O'Leary
- 29-30 A Practical Guide to Encryption and Certificate Authorities, John O'Leary

December

- Ontario, CA**
- 3-4 Practical Forensics: How to Manage IT Investigations, Peter Garza
- 5-7 Technical Recovery of Electronic Evidence (Hands-on), Peter Garza



For address change or other subscriber information please call Member Services, at: 415-947-6330

Director: Patrice Rapalus	415-947-6370
Editorial Director: Richard Power	415-947-6371
Education Director: John O'Leary	972-596-6384
Marketing Manager: Nancy Baer	415-947-6364
National Sales Manager: Cynthia Deno	831-335-9445
Special Projects: Pam Salaway	631-878-2205
Production: Rosie Jung	415-947-6366
Membership Services: Rachel Elder	415-947-6367
Conference Staff:	415-947-6320
Tobbe Sikorski, <i>Conference Manager</i>	415-947-6373
Kimber Heald, <i>Registration Manager</i>	415-947-6372
Joanna Kaufman, <i>Project Coordinator</i>	415-947-6369

Fax 415-947-6023
Hotline 415-947-6371

E-mail: All CSI staff members can be reached via e-mail—use the first letter of first name and complete last name @cmp.com. (i.e., prapalus@cmp.com)

WWW: <http://www.gocsi.com>

Copyright ©2001, Computer Security Institute, 600 Harrison St., San Francisco, CA 94107. All rights reserved. Reproduction in any form is forbidden without express permission of copyright owner. *Computer Security ALERT* is sent monthly to members of the Computer Security Institute.